PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-162693

(43)Date of publication of application : 23.06.1995

(51)Int.Cl. H04N 1/44
G09C 1/04
H04L 9/06
H04L 9/14
H04N 1/32

(21)Application number : 05-311971

(22)Date of filing : 13.12.1993

(71)Applicant : RICOH ELEMEX CORP

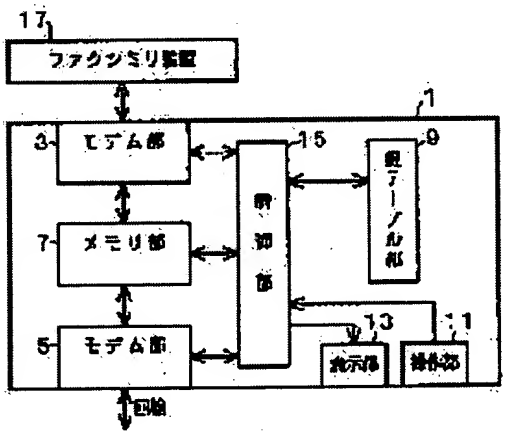
(72)Inventor : SAKA YASUHIKO

(54) CIPHERED MULTI-ADDRESS DATA TRANSMITTER-RECEIVER AND ADAPTER

(57)Abstract:

PURPOSE: To transmit the same shortest ciphered sentence to plural reception destinations by converting data for transmission to the ciphered sentence by a common key and ciphering the common key by individual keys corresponding to the respective reception destinations.

CONSTITUTION: A control part 15 controls respective parts and performs processings such as the working of the data and the transmission and reception, etc. Reception destination titles stored in a key table part 9 are turned to a menu, displayed at a display part 13 and selected by an operator. In the key table part 9, an individual key table composed of reception destination codes, the individual keys and the reception destination titles is stored. Then, the data are ciphered by the common key and the common key is stored in the control part 15 or the key table part 9 and functions similarly to the individual keys. The common key is used, a prescribed arithmetic operation is performed and the data inputted from a facsimile equipment 17 to a memory part 7 are stored in the memory part 7 again. From the stored data, the table of the ciphered common key and the reception destination code for performing transmission thereafter is prepared and is transmitted along with the data.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of

rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－162693

(43)公開日　平成７年(1995)６月23日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｎ	1/44		7251－5C		
Ｇ０９Ｃ	1/04		9364－5L		
Ｈ０４Ｌ	9/06				
	9/14				
				Ｈ０４Ｌ　9/ 02　Ｚ	

審査請求　未請求　請求項の数４　ＯＬ　（全 ９ 頁）　最終頁に続く

(21)出願番号　特願平5－311971

(22)出願日　平成５年(1993)12月13日

(71)出願人　000006932
リコーエレメックス株式会社
愛知県名古屋市東区泉２丁目28番24号

(72)発明者　坂　康彦
愛知県名古屋市東区泉２丁目28番24号　リコーエレメックス株式会社内

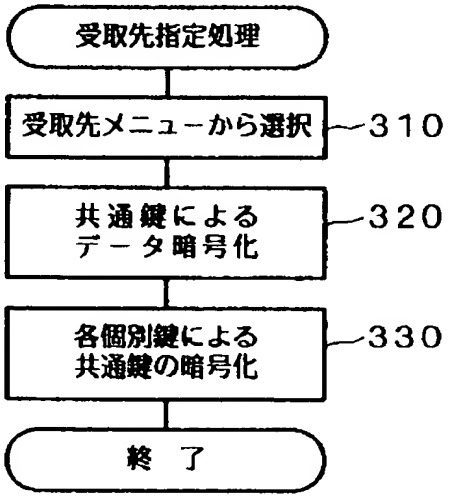
(74)代理人　弁理士　足立　勉

(54)【発明の名称】　暗号化同報データ送受信装置およびアダプタ

(57)【要約】

【目的】　複数の受取先に暗号化した同一文章をできるだけ短くして送信したい。

【構成】　送信側では、メモリ部７にファクシミリ装置１７から入力されたデータを、共通鍵を用いて所定の演算を実行することにより、暗号化する（ステップ３２０）。次にステップ３１０で選択された受取先に対応する個別鍵を個別鍵テーブルから順次読み出し、その個別鍵にて共通鍵を暗号化演算し、受取先符号とともにメモリ部７に格納する（ステップ３３０）。この格納データの内から、これから送信する受取先符号と暗号化共通鍵とのテーブルを作成し、データ暗号文の先頭に配置して一組のデータとする。このデータを送信する。受信側では受取先の要求毎に共通鍵を復号し、次に共通鍵でデータを復号して受取先に渡す。



1

【特許請求の範囲】

【請求項１】　暗号化されたデータを送信する暗号化同報データ送信装置であって、

送信用データを共通鍵に基づき暗号文に変換する暗号化手段と、

上記送信用データを受け取る受信先を複数指示可能な指示手段と、

上記受取先の各々に対応する個別鍵で、上記共通鍵を暗号化し、個別鍵の数に対応する共通鍵暗号文を得る共通鍵暗号化手段と、

上記暗号文と、上記個別鍵の数に対応する複数の共通鍵暗号文と、上記受信先の各々に対応する複数の識別符号とを一組として送信する送信手段と、

を備えたことを特徴とする暗号化同報データ送信装置。

【請求項２】　送信装置からデータを受け取り、このデータを暗号化して送信する暗号化同報データ送信用アダプタであって、

送信装置からのデータまたは該データに対して所定処理を行ったデータを、共通鍵に基づき暗号文に変換する暗号化手段と、

上記データを受け取る受信先を複数指示可能な指示手段と、

上記受取先の各々に対応する個別鍵で、上記共通鍵を暗号化し、個別鍵の数に対応する共通鍵暗号文を得る共通鍵暗号化手段と、

上記暗号文と、上記個別鍵の数に対応する複数の共通鍵暗号文と、上記受信先の各々に対応する複数の識別符号とを一組として送信する送信手段と、

を備えたことを特徴とする暗号化同報データ送信用アダプタ。

【請求項３】　請求項１記載の暗号化同報データ送信装置または請求項２記載の暗号化同報データ送信用アダプタからのデータを受信する暗号化同報データ受信装置であって、

受取先が入力される受取入力手段と、

上記受取入力手段に入力された受取先に対応する識別符号が受信データ中に存在する場合に、その受取先に対応する個別鍵に基づき、受信データ中に存在する共通鍵暗号文を復号して、共通鍵を取り出す共通鍵復号手段と、

上記共通鍵復号手段にて復号された共通鍵に基づき、受信データ中に存在する暗号文を復号する復号手段と、

を備えたことを特徴とする暗号化同報データ受信装置。

【請求項４】　請求項１記載の暗号化同報データ送信装置または請求項２記載の暗号化同報データ送信用アダプタからのデータを受信し所定の処理の後、受信装置に送信する暗号化同報データ受信用アダプタであって、

受取先が入力される受取入力手段と、

上記受取入力手段に入力された受取先に対応する識別符号が受信データ中に存在する場合に、その受取先に対応する個別鍵に基づき、受信データ中に存在する共通鍵暗号文を復号して、共通鍵を取り出す共通鍵復号手段と、

上記共通鍵復号手段にて復号された共通鍵に基づき、受信データ中に存在する暗号文を復号する復号手段と、

を備えたことを特徴とする暗号化同報データ受信用アダプタ。

2

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、ファクシミリ装置等のデータ送受信装置およびアダプタに関し、特に暗号文の同報通信に関する。

【０００２】

【従来の技術】ファクシミリ装置の通信内容を秘匿するため、送信側ではデータを暗号化してから送信し、受信側では暗号化されたデータを受け取ってから復号して用紙等に出力する機能が知られている。このような機能を有するファクシミリ装置において、更に同報機能を有するファクシミリ装置がある。同報機能とは同一のデータを複数の受取先に伝送する機能である。

【０００３】この同報機能の内で、一台のファクシミリ装置に対して同一データを暗号化してから伝送し、その一台のファクシミリ装置から複数の受取人の要求がある毎に、個々に復号して出力するシステムがあった。この送受信処理は例えば次のように行われていた。

【０００４】即ち、一つのデータを、受信者毎に与えられている個別鍵に基づいて、個々に暗号文を算出し、その受信者に対応した数の暗号文を全て、一台のファクシミリ装置に送信していた。受信側のファクシミリでは、受信者数分の全ての暗号文を受け取って一旦メモリに記憶し、その内容を、各受信者が暗唱番号やカード等をファクシミリに入力することを条件に、各受信者用の個別鍵にて暗号化されているデータを復号して出力していた。このことにより、データの秘匿が保たれていた。

【０００５】

【発明が解決しようとする課題】しかし、伝送する文書は同一であり、受け取るファクシミリ装置も同一であるにもかかわらず、受信者毎に異なる個別鍵を用いて暗号化を実施するために、元のデータは同一でも暗号文がことなってしまい、送信側も受信側も受信者の数だけの暗号文を送受信しなくてはならなかった。さらに受信側は、受信者が引き出すまで秘匿しておかなくてはならないため、複数の暗号文を一旦記憶するためのメモリも確保しなくてはならなかった。

【０００６】

【課題を解決するための手段】請求項１記載の暗号化同報データ送信装置は、図１に例示するごとく、暗号化されたデータを送信する暗号化同報データ送信装置であって、送信用データを共通鍵に基づき暗号文に変換する暗号化手段と、上記送信用データを受け取る受信先を複数指示可能な指示手段と、上記受取先の各々に対応する個別鍵で、上記共通鍵を暗号化し、個別鍵の数に対応する

共通鍵暗号文を得る共通鍵暗号化手段と、上記暗号文と、上記個別鍵の数に対応する複数の共通鍵暗号文と、上記受信先の各々に対応する複数の識別符号とを一組として送信する送信手段と、を備えたことを特徴とする。

【０００７】請求項２記載の暗号化同報データ送信用アダプタは、図２に例示するごとく、送信装置からデータを受け取り、このデータを暗号化して送信する暗号化同報データ送信用アダプタであって、送信装置からのデータまたは該データに対して所定処理を行ったデータを、共通鍵に基づき暗号文に変換する暗号化手段と、上記データを受け取る受信先を複数指示可能な指示手段と、上記受取先の各々に対応する個別鍵で、上記共通鍵を暗号化し、個別鍵の数に対応する共通鍵暗号文を得る共通鍵暗号化手段と、上記暗号文と、上記個別鍵の数に対応する複数の共通鍵暗号文と、上記受信先の各々に対応する複数の識別符号とを一組として送信する送信手段と、を備えたことを特徴とする。

【０００８】請求項３記載の暗号化同報データ受信装置は、図３に例示するごとく、請求項１記載の暗号化同報データ送信装置または請求項２記載の暗号化同報データ送信用アダプタからのデータを受信する暗号化同報データ受信装置であって、受取先が入力される受取入力手段と、上記受取入力手段に入力された受取先に対応する識別符号が受信データ中に存在する場合に、その受取先に対応する個別鍵に基づき、受信データ中に存在する共通鍵暗号文を復号して、共通鍵を取り出す共通鍵復号手段と、上記共通鍵復号手段にて復号された共通鍵に基づき、受信データ中に存在する暗号文を復号する復号手段と、を備えたことを特徴とする。

【０００９】請求項４記載の暗号化同報データ受信用アダプタは、図４に例示するごとく、請求項１記載の暗号化同報データ送信装置または請求項２記載の暗号化同報データ送信用アダプタからのデータを受信し所定の処理の後、受信装置に送信する暗号化同報データ受信用アダプタであって、受取先が入力される受取入力手段と、上記受取入力手段に入力された受取先に対応する識別符号が受信データ中に存在する場合に、その受取先に対応する個別鍵に基づき、受信データ中に存在する共通鍵暗号文を復号して、共通鍵を取り出す共通鍵復号手段と、上記共通鍵復号手段にて復号された共通鍵に基づき、受信データ中に存在する暗号文を復号する復号手段と、を備えたことを特徴とする。

【００１０】

【作用】請求項１記載の暗号化同報データ送信装置および請求項２記載の暗号化同報データ送信用アダプタは、暗号化手段により、データを共通鍵に基づき暗号文に変換する。共通鍵は全ての送信用データの暗号化に用いられる鍵であるので、この共通鍵にて作成された暗号文は、元のデータが同一で有れば、同一の暗号文となる。したがって、同報したい受取先には一つの暗号文でよいことになる。

【００１１】ただし、共通鍵が全ての受取先に対して共通であるので、共通鍵暗号化手段にて、受取先の各々に対応する個別鍵で、共通鍵を暗号化し、個別鍵の数に対応する複数の共通鍵暗号文を得、送信手段にて、暗号文と、個別鍵の数に対応する複数の共通鍵暗号文と、受信先の各々に対応する複数の識別符号とを一組として送信する。

【００１２】暗号化された複数の共通鍵については受信先の数だけ存在することになるが、このような鍵の暗号文は極めて短いものであり、データ量に大きな影響はない。識別符号についても同様である。したがって、一組の送信用データ内に、暗号文は１つでよいことになり、送信データ量やその処理が過大にならない。

【００１３】このため、請求項３記載の暗号化同報データ受信装置および請求項４記載の暗号化同報データ受信用アダプタ側では、受信するデータはきわめて短いものとなる。また受信時におけるデータの記憶も少ないメモリ消費で済む。受取入力手段に入力された受取先に対応する識別符号が受信データ中に存在する場合に、共通鍵復号手段が、その受取先の個別鍵に基づき、受信データから該当する共通鍵暗号文を復号して共通鍵を取り出す。更に、この共通鍵に基づき、復号手段が受信データ中に存在する暗号文を復号する。

【００１４】

【実施例】第１実施例として、図５に暗号化同報データ送受信用アダプタを使用した暗号化同報データ送受信システムのブロック図を示す。アダプタ１は、２つのモデム部３，５、メモリ部７、鍵テーブル部９、操作部１１、表示部１３および制御部１５を備えている。一方のモデム部３は直結されているファクシミリ装置１７との間のデータ伝送を仲介し、他方のモデム部５は回線に接続されている。メモリ部７はモデム部３，５から入力されるデータを直接記憶したり、逆に記憶されているデータを直接モデム部３，５へ出力している。鍵テーブル部９は個別鍵を受取先と関係付けて記憶している。操作部１１は各種のキーを備え、オペレータの指示を入力する。表示部１３は必要なメッセージをオペレータに伝達する。制御部１５はＣＰＵ、ＲＯＭ、ＲＡＭ、Ｉ／Ｏ等を備え、マイクロコンピュータとして構成されている。尚、この構成以外に、電源回路等の構成が存在するが、本実施例の機能を説明するための要部ではないので、図示省略する。

【００１５】制御部１５により、上記各部が制御されて、データ加工やその送受信等の処理が実施される。図６はその主たる処理を表している。本処理は繰り返し実行される。まず、処理が開始されると、回線からモデム部５を介してメモリ部７へ入力されたデータが存在するか否かが判定される（ステップ１００）。例えば、全くメモリ部７へはデータが入力されていない状態、あるい

は回線から入力されている途中の状態では、「ＮＯ」と判定される。次に、指示入力が有ったか、その内容は何かが判定される（ステップ２００）。操作部１１から「受取先指定」の指示入力があれば、受取先指定処理（ステップ３００）が実行されて必要なだけの受取先が指定され、次いで終了して最初の処理（ステップ１００）に戻る。

【００１６】ここで、受取先指定処理（ステップ３００）の詳細を図７にて説明する。まず鍵テーブル部９に記憶されている受取先名称をメニュー化して表示部１３に表示し、オペレータに選択させる（ステップ３１０）。鍵テーブル部９には図１０に示すごとくの受取先符号、個別鍵および受取先名称からなる個別鍵テーブルが格納されている。受取先符号は受取先に対応して設けられているものであり、極めて少ないビット数のデータからなるので、具体的に表されている受取先名称の代わりに用いられるものである。勿論、受取先名称そのものを受取先符号として用いても良い。個別鍵は受取先毎に設定されている鍵である。鍵は所定ビットのデータからなり、暗号化したいイメージデータに対して所定のアルゴリズムで演算処理されることにより、イメージデータを暗号化するものである。

【００１７】ステップ３１０では、この内の受取先名称をリストとして表示して、オペレータに選択させているが、単数選択してもよいし複数選択してもよい。次に共通鍵によるデータ暗号化が行われる（ステップ３２０）。この共通鍵は制御部１５あるいは鍵テーブル部９に格納されているものであり、上記個別鍵と同様な働きをするものである。即ち、メモリ部７にファクシミリ装置１７から入力されたデータを、共通鍵を用いて所定の演算を実行することにより、暗号化する。暗号化されたデータは再度メモリ部７に格納される。

【００１８】次に、ステップ３１０で選択された受取先に対応する個別鍵を個別鍵テーブルから順次読み出し、その個別鍵にて共通鍵を暗号化演算し、受取先符号とともにメモリ部７に格納する（ステップ３３０）。従って、この時、メモリ部７には図１１（Ａ）に示す受取先符号と暗号化共通鍵とが組になったテーブルＴｋと、一つのデータ暗号文Ｔｓとが存在することになる。

【００１９】図６に戻り、次に指示入力が「送信」であった場合には、メモリ部７に送信用データが存在するか否かが判定される（ステップ４００）。例えば、全くメモリ部７へは図１１（Ａ）に示すデータが存在しない状態では、「ＮＯ」と判定される。そしてこのまま処理を終了し最初の処理（ステップ１００）に戻る。

【００２０】送信用データが存在する場合、即ち、オペレータがファクシミリ装置１７に原稿の読取操作を実施することにより、ファクシミリ装置１７側からデータが送られていれば、送信処理が行われる（ステップ５００）。送信処理の詳細を図８に示す。

【００２１】まず、操作部１１からの送信先ファクシミリ番号の入力待となる（ステップ５１０）。入力されれば、次に表示部１３に、受取先名称が表示され、この表示された受取先名称の選択待となる（ステップ５２０）。このときの受取先名称は、図１１（Ａ）に示すテーブルＴｋに示した受取先符号に対応する名称、即ち、ステップ３１０で選択された受取先名称であり、図１０に示した個別鍵テーブルから抽出される。

【００２２】ここで例えば、４つの受取先が選択されたとすると、次にヘッダを作成する（ステップ５３０）。即ち、選択した４つの受取先に対応する符号Ａ1，Ａ3，Ａ10，Ａ25と各々暗号化した共通鍵Ｓ1，Ｓ3，Ｓ10，Ｓ25とのテーブルを作成し、データ暗号文Ｔｓの先頭にヘッダHd1として配置し、図１１（Ｂ）に示す一組のデータＤs1とする処理が行われる。

【００２３】次にこのデータＤs1を、モデム部５および回線を介して送信相手のファクシミリ装置に向けて送信する（ステップ５４０）。この送信の際には、一般的なファクシミリ装置が実行している送信手順で行われる。こうして処理を終了し、再度ステップ１００の処理に戻る。

【００２４】同一のデータを別のファクシミリ装置に送信したいときには、再度ステップ２００で「送信」を選択し、ステップ５１０，５２０にて別のファクシミリ装置の番号および受取先を選択すればよい。例えば、新たに符号Ａ2，Ａ99に該当する受取先を選択すれば、上述したごとくの処理にて図１１（Ｃ）に示すヘッダHd2とデータ暗号文Ｔｓとの一組のデータＤs2が作成され、別のファクシミリ装置に送信される。

【００２５】尚、ステップ２００では、他の各種処理、例えば図１０に示した個別鍵テーブルに追加するための処理等が選択でき、ステップ６００にて実施される。次に、回線を介して他のファクシミリ装置からのデータが受信された場合について説明する。図１１（Ｂ），（Ｃ）に示した形式のデータをモデム部５が受信すると、メモリ部７の該当個所に記憶される。

【００２６】この記憶の完了後ステップ１００にて「ＹＥＳ」と判定され、復号処理（ステップ７００）が開始される。復号処理の詳細を図９に示す。まず、受取要求が有るか否かが判定される（ステップ７１０）。この要求は、操作部１１への所定のＩＤやパスワードの入力、あるいは受取先別ＩＤカードが図示しないカード読取部に差し込まれたことにより、要求有りと判定される。要求がなされていなければ、このまま復号処理を終了し、ステップ２００の処理に移る。したがって受信していても要求がなければ、復号はなされない。

【００２７】受取要求が有った場合、ステップ７１０にて「ＹＥＳ」と判定され、メモリ部７に記憶されているデータのヘッダHd1中に要求に合致する受取先符号が存在するか否かを判断する（ステップ７２０）。無ければ

「ＮＯ」と判定され、復号処理を終了してステップ２００の処理に移る。

【００２８】合致する受取先符号が存在すると、次に鍵テーブル部９からその符号に対応する個別鍵を読み出す（ステップ７３０）。例えば、合致した符号が符号Ａ3であった場合には、図１０に示したテーブルから個別鍵Ｐ3を読み出す。次にこの個別鍵Ｐ3を用いて、データ中の暗号化された共通鍵を復号演算する（ステップ７４０）。例えば受信したデータが図１１（Ｂ）に示したデータＤs1であった場合、共通鍵暗号文Ｓ3が復号されることになる。

【００２９】こうして、復号した共通鍵を用いて、データ暗号文Ｔsを復号演算する（ステップ７５０）。次に直結しているファクシミリ装置１７へモデム部３を介して通常のファクシミリ通信として復号されたデータ暗号文を送信する（ステップ７６０）。勿論、通常のファクシミリ通信であるので、圧縮・伸長処理が介在する場合もある。尚、アダプタ１は、復号されたデータに、図１０に示したテーブルから得られる受取先名称を付加してファクシミリ装置１７へ送信してもよい。更に受信時間等の付属データを付加してもよい。

【００３０】ファクシミリ装置１７側では、このデータをイメージデータとして受信しプリントアウトする。このことにより、直ちに受取要求した者に印刷物が渡される。他の受取先が受取要求すれば、上述の復号処理（ステップ７００）が繰り返される。例えば、受取先符号Ａ25の者が受取要求すれば、個別鍵Ｐ25により共通鍵暗号文Ｓ25が復号され、この共通鍵を用いて同一のデータ暗号文Ｔsが復号演算される。こうして、秘密を維持された状態で受信され、かつ保存されるとともに、復号されたデータは直ちに正式な受取先にのみ渡されることになる。

【００３１】尚、全ての受取先に対して復号されたデータが出力されれば、データＤs1は消去される。また復号が全ての受取先に対して出力されていない場合に、次のデータが受信されれば、それもメモリ部７の別の領域に記憶され、ステップ７２０での検索対象となる。

【００３２】尚、本アダプタ１は、この他の機能として、データの送信エラーをチェックするためのパリティを送信データに付加したりすることができ、更に、一般的なファクシミリ装置が有している機能も有することができる。上述したごとく、本実施例は同一ファクシミリ装置の複数の受取先に対しては、データ暗号文は一つで済む。また、受取先の数だけヘッダとして付加される受取先符号および共通鍵暗号文は元来短いものであることから、全体として極めて短い暗号を送受信するだけで、複数の受信先に同一文書を秘密状態で伝達できる。

【００３３】次に、ファクシミリ装置に上記アダプタ１の機能を一体化した第２実施例について説明する。図１２に示すごとく、本実施例のファクシミリ装置８００は、読取部８０２、操作部８０４、表示部８０６、記録部８０８、メモリ部８１０、モデム部８１２、鍵テーブル部８１４および制御部８１６を主たる構成としている。

【００３４】読取部８０２は原稿に表示されたイメージをビットデータとして読み取り、所定の圧縮等の処理を行う。操作部８０４は各種のキーを備え、オペレータの指示を入力する。表示部８０６は必要なメッセージをオペレータに伝達する。記録部８０８はメモリ部８１０内のデータを印刷物として出力する。メモリ部８１０はモデム部８１２から入力されるデータを直接記憶したり、逆に読取部８０２からのデータを直接モデム部８１２へ出力している。モデム部８１２は回線に接続されて信号を入出力する。鍵テーブル部８１４は前記第１実施例と同じ機能を有する。制御部８１６はＣＰＵ、ＲＯＭ、ＲＡＭ、Ｉ／Ｏ等を備え、マイクロコンピュータとして構成され、読取部８０２、操作部８０４、表示部８０６、記録部８０８、メモリ部８１０、モデム部８１２および鍵テーブル部８１４を制御して、通常のファクシミリ装置としての機能を実現している。更に鍵テーブル部８１４は第１実施例の制御部１５と同様に、図６に示したフローチャートと同等の機能も実現している。したがってステップ７６０の処理が、記録部８０８への復号化データの出力である点が異なる。効果は第１実施例と同じである。

【００３５】上記各実施例において、共通鍵の暗号化・復号化は個別鍵に基づいて行うが、この他に送信側のファクシミリ装置あるいはアダプタが有している個別鍵と、受信側のファクシミリ装置あるいはアダプタが有している個別鍵との両者を使用してもよい。またこの暗号化・復号化の演算は、送受信側が有する同一の秘密のアルゴリズムにしたがって計算させてもよい。

【００３６】本発明は上記各実施例に限られることなく、その要旨を変更しない限り、他の種々の態様で実施することが可能である。例えば、本暗号化同報データ送受信装置およびアダプタは、ファクシミリ装置に限らず各種デジタル通信装置が含まれる。

【００３７】

【発明の効果】送信において、データを暗号文に変換する共通鍵は、全ての送信用データの暗号化に用いられる鍵であるので、この共通鍵にて作成された暗号文は、元のデータが同一で有れば、同一の暗号文となる。したがって、同報したい受取先には一つの暗号文でよいことになる。暗号化された共通鍵については受信先の数だけ複数存在することになるが、このような鍵の暗号文は極めて短いものであり、データ量に大きな影響はない。識別符号についても同様である。したがって、一組の送信用データ内に、暗号文は１つでよいことになり、送信データ量やその処理が過大にならない。

【００３８】このため、受信側においても、受信するデ

9

ータはきわめて短いものとなる。また受信時におけるデータの記憶も少ないメモリ消費で済む。

【図面の簡単な説明】

【図１】　請求項１記載の発明の構成例示図である。

【図２】　請求項２記載の発明の構成例示図である。

【図３】　請求項３記載の発明の構成例示図である。

【図４】　請求項４記載の発明の構成例示図である。

【図５】　暗号化同報データ送受信システムの第１実施例説明用ブロック図である。

【図６】　アダプタ側処理のフローチャートである。

【図７】　受取先指定処理のフローチャートである。

【図８】　送信処理のフローチャートである。

【図９】　復号処理のフローチャートである。

【図１０】　個別鍵テーブルの構造説明図である。

【図１１】　データ構造説明図であり、（Ａ）は暗号化演算により得られたデータ構造説明図、（Ｂ）および

10

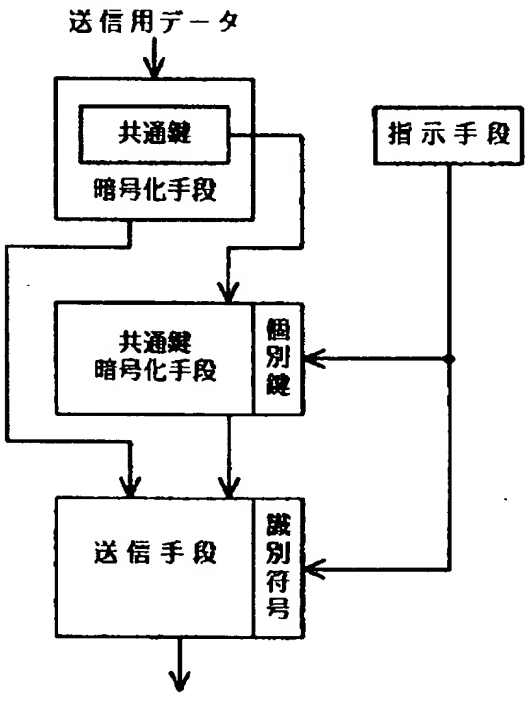
（Ｃ）はその送信用データあるいは受信用データ説明図である。

【図１２】　第２実施例のファクシミリ装置のブロック図である。

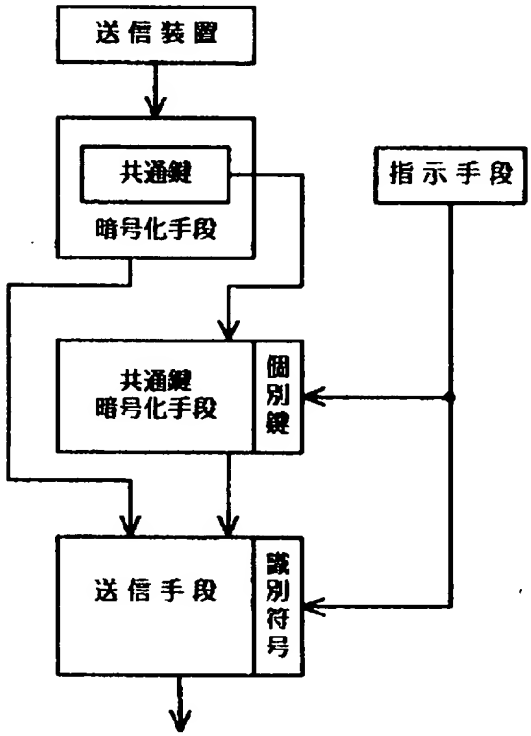
【符号の説明】

１・・・アダプタ、３・・・モデム部、５・・・モデム部、７・・・メモリ部、９・・・鍵テーブル部、１１・・・操作部、１３・・・表示部、１５・・・制御部、１７・・・ファクシミリ装置、８００・・・ファクシミリ装置、８０２・・・読取部、８０４・・・操作部、８０６・・・表示部、８０８・・・記録部、８１０・・・メモリ部、８１２・・・モデム部、８１４・・・鍵テーブル部、８１６・・・制御部、Ds1，Ds2・・・一組のデータ暗号文、Ｔs・・・データ暗号文、Ｔk・・・暗号化共通鍵テーブル

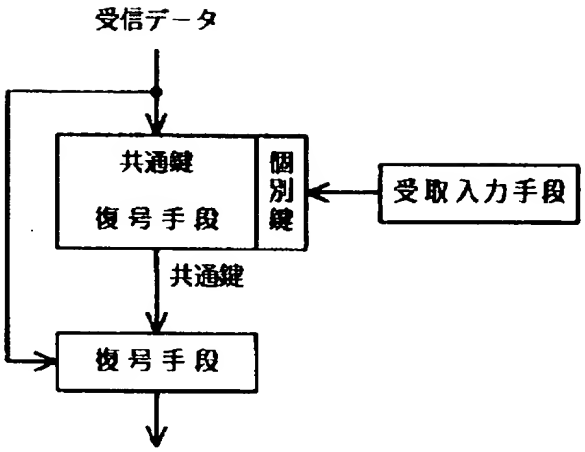
【図１】



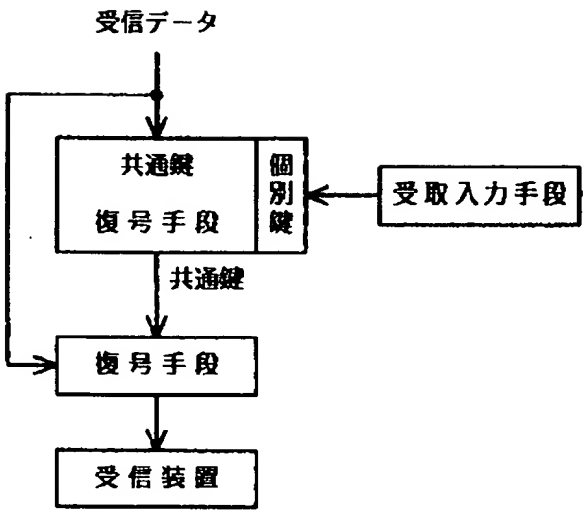
【図２】



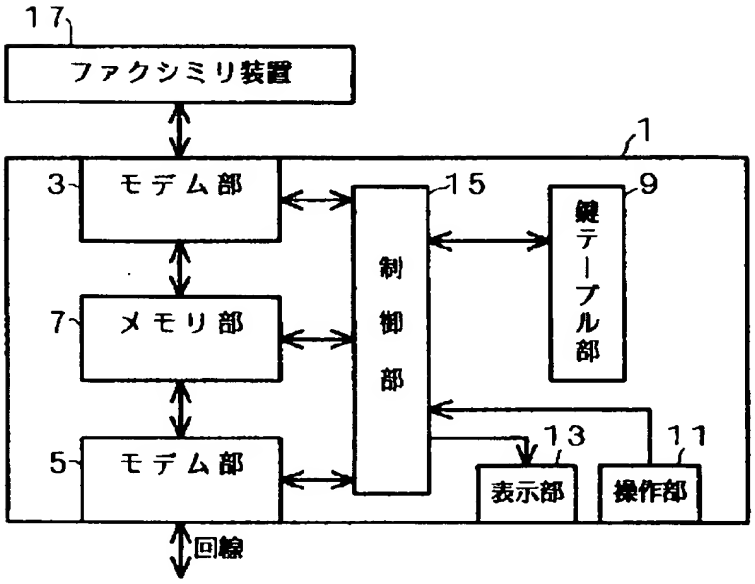
【図３】



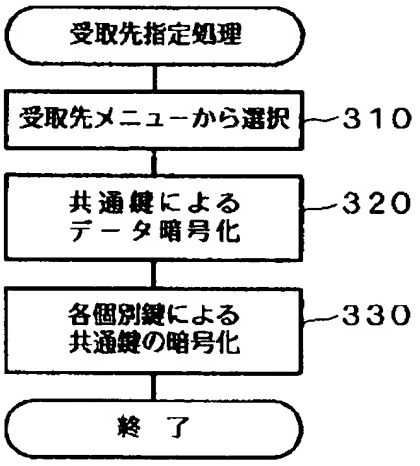
【図４】



【図５】



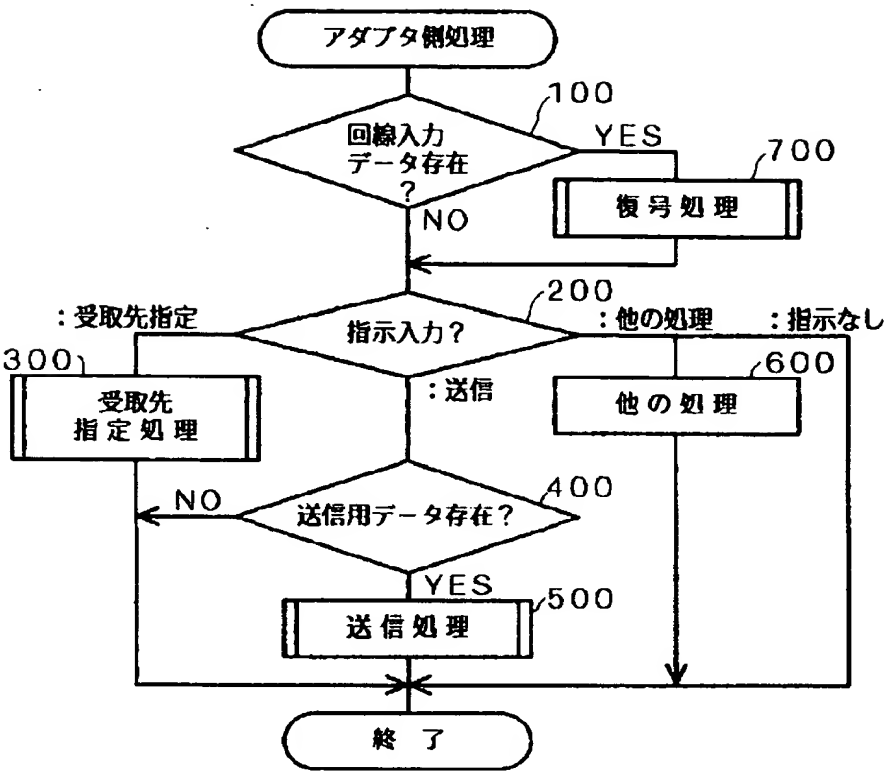
【図７】



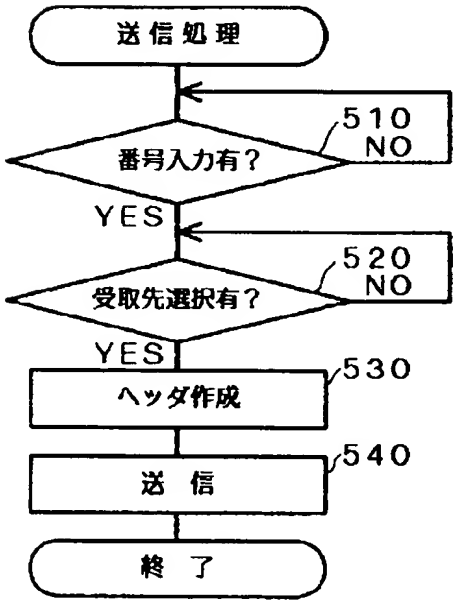
【図１０】

受取先符号	個別鍵	受取先名称
A1	P1	○○○部長
A2	P2	△△△課長
A3	P3	×××課長
A4	P4	□□□係長
A5	P5	○×△係長
A6	P6	○×○係長
A7	P7	×○×
⋮		

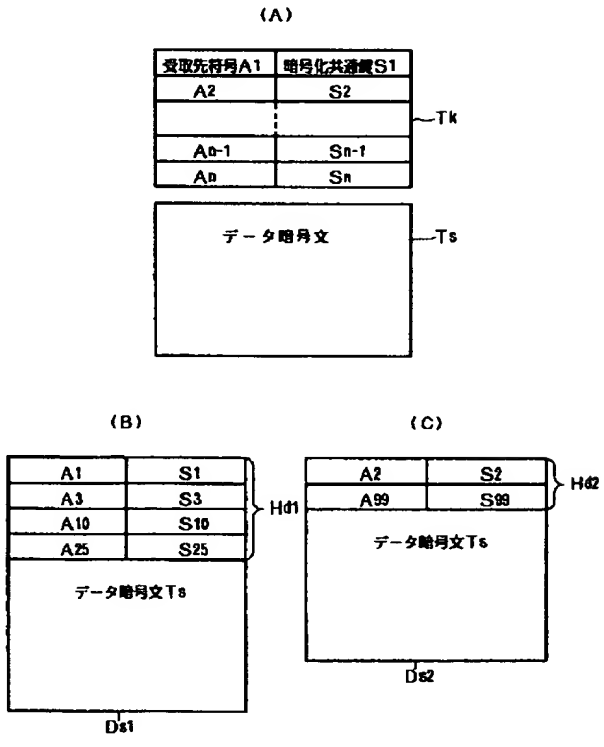
【図６】


アダプタ側処理
100
回線入力データ存在？
YES
NO
700
復号処理
200
：受取先指定
指示入力？
：他の処理
：指示なし
300
受取先指定処理
：送信
600
他の処理
NO
400
送信用データ存在？
YES
500
送信処理
終了

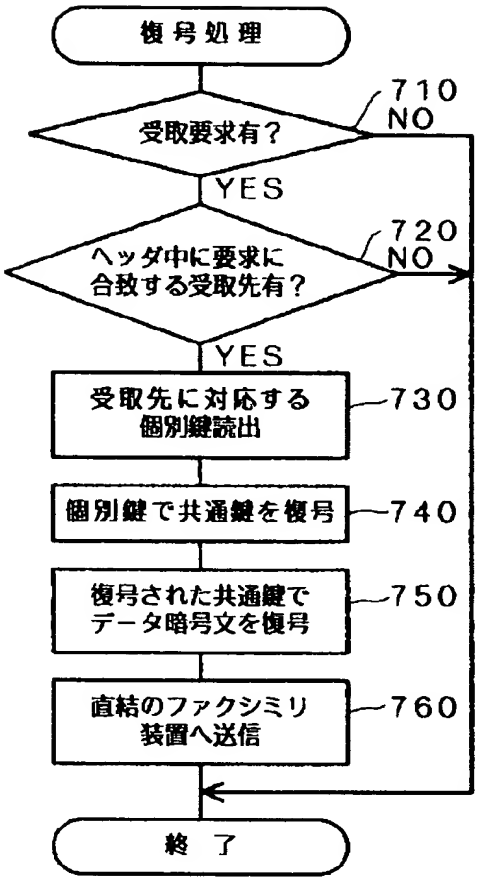
【図８】


送信処理
510
番号入力有？
NO
YES
520
受取先選択有？
NO
YES
530
ヘッダ作成
540
送信
終了

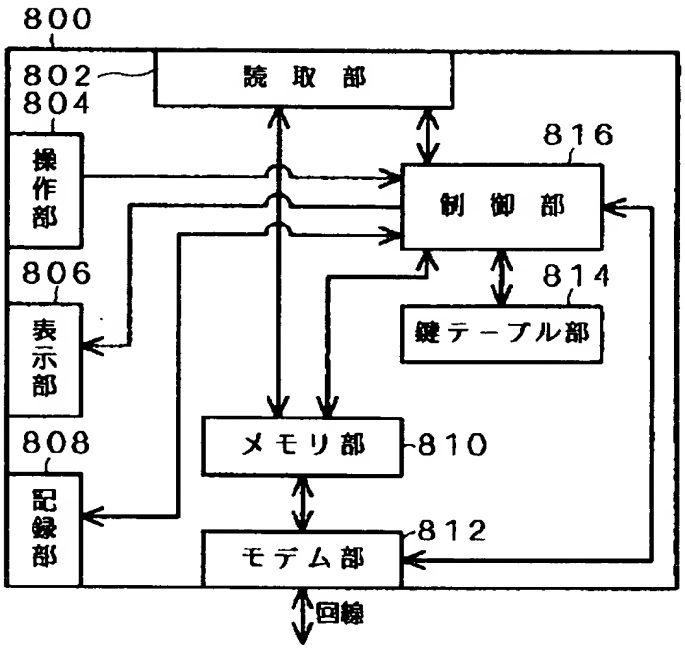
【図１１】


(A)
受取先符号A1
暗号化共通鍵S1
A2
S2
An-1
Sn-1
An
Sn
Tk
データ暗号文
Ts
(B)
A1
S1
A3
S3
A10
S10
A25
S25
Hd1
データ暗号文Ts
Ds1
(C)
A2
S2
A99
S99
Hd2
データ暗号文Ts
Ds2

【図９】



【図１２】



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｎ　1/32		Ｈ　7251－5Ｃ		